UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,404	06/13/2000	Nicolas J. Hammond	14102.0002	5767

23859 7590 01/07/2005

NEEDLE & ROSENBERG, P.C.
SUITE 1000
999 PEACHTREE STREET
ATLANTA, GA 30309-3915

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/592,404	HAMMOND, NICOLAS J.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) *9* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed 02 July 2004 has been noted and made of record.

2. Claims 1-47 have been presented for examination.

3. Claim 9 has been cancelled as per Applicant's request.

Response to Arguments

4. Applicant's arguments with respect to claims 1-9 and 11-47 have been considered but are moot in view of the new ground(s) of rejection.

5. See further rejections that follow.

Specification

6. The language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thereby, defining "a" as a term of singularity.

7. The Specification is objected to due to page 4 where the Applicant tries to define "a" to include plural references.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 10 and 24-47 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The Applicant

claims recording the scheduled security audit scan in a database, and there is insufficient support in the Specification for such a claim limitation. *In re Wands,* 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1998). See also MPEP § 2164.01(a) and § 2164.04.

Claim Rejections - 35 USC § 103

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-6, 14, 21, 23, 26, 31, 36, 40, 45, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,205,552 to Fudge, hereinafter Fudge, in view of U.S. Patent No. 6,347,374 to Drake et al., hereinafter Drake, and further in view of 6,185,689 to Todd, Sr. et al, hereinafter Todd, and U.S. Patent No. 6,517,587 to Satyavolu et al., hereinafter Satyavolu.

12. As per claim 1, Fudge teaches an apparatus for auditing security of a remote computer system, comprising:

b. a scanning machine in communication with the global computer network and programmed to execute selectively a security audit scan of the remote computer system via the global computer network, each scanning machine capable of conducting multiple types of security assessments (Figure 1 [block 160]; column 3, lines 47-59); and

c. a central computer, having a memory, configured as a database server, in communication with the secure application server and the scanning machine (Figures 1 [block 120], 2 [blocks 212, 214, 218]; column 3, lines 19-33; column 4, lines 21-41; column 4, lines 61-67), programmed to perform operations comprising:

a. evaluating a database (Figure 1 [block 152]; column 3, lines 56-59; column 4, line 35-42; column 4, lines 61-67);

c. copying scan-related information into one of the available scanning machines and instructing the scanning machine to begin the security audit scan (Figures 2 [block 218], 3 [blocks 304, 306]; column 4, lines 47-54); and

d. recording the results of the security audit scan in the memory (Figure 3 [block 306]; column 4, lines 47-54).

13. Fudge does not disclose a plurality of scanning machines. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a plurality of scanning machines [Drake, column 1, lines 4-10], since Drake states at column 2, lines 19-24 that such a modification would aid in detecting abnormal computer actions constituting intrusions of insiders and detect intruding outsiders. Additionally, it has been held in the art that it requires only routine skill to duplicate a part for it to have a multiple effect. See MPEP § 2144.04; see also *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

14. Fudge and Drake do not disclose a secure application server in communication with a global computer network and programmed to receive selectively security audit instruction data from the remote computer system via the global computer network. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a secure application server in communication with a global computer network and programmed to receive selectively security audit instruction data from the remote computer system via the global computer network [Todd, Figures 1 [block 26], 2 [blocks 34, 38], 3 [block 32]; column 4, lines 7-19; column 6, lines 14-26], since Todd states at column 3, line 62 to column 4, line 4 that such

a modification would provide a service that can be operated conveniently and securely from a World Wide Web browser at an arbitrary host, that fully assess file access, version information, and vulnerability to denial of service attacks, and has sufficient security to minimize the danger of exploitation by hackers to obtain offensive information.

15. Fudge, Drake, and Todd do not disclose a scheduler, evaluating the database to determine if the security audit is currently scheduled to be run on one of the scanning machines, and determining which of the plurality of scanning machines is available to perform a security audit scan by examining a schedule for each scanning machine to identify certain ones of the scanning machines that are conducting another security audit scan or are scheduled to conduct another security audit scan, the available scanning machines comprising all of the scanning machines except for the certain scanning machines. It would have been to one of ordinary skill in the art at the time the invention was made to include the central computer as a scheduler [Satyavolu, Figure 1 [block 115], column 5, line 55 to column 6, line 7], evaluating a database to determine if there is an event currently scheduled to be run on one of the machines [Satyavolu, Figure 1 [block 127], column 6, lines 7-34], and a determining step to determine which machine is available to execute the gathering of information [Satyavolu, Figure 1 [block 127], column 6, lines 7-34], since Satyavolu discloses at column 2, lines 26-36 that such a modification would allow a large number of cooperating computer-nodes to fulfill a number of automatically-scheduled and user-initiated data requests in a wholly automated and transparent fashion.

16. Regarding claim 2, Todd teaches wherein the secure application server comprises a Web server (column 6, lines 14-17).

17. Regarding claims 3, 14, 31, and 40, Todd teaches wherein the central computer is further programmed to issue a notification the security audit scan is commencing (Figures 3 [block 42], 7 [block 42]; column 6, lines 40-49).

18. Regarding claims 4, 21, 36, and 45, Fudge teaches wherein the central computer is further programmed to update the database to indicate that the security audit scan is complete (Figure 1 [blocks 150, 152]; column 3, lines 56-59; column 4, lines 61-67).

19. Regarding claims 5, 23, and 47, Todd teaches wherein the central computer is further programmed to send a signal representing completion of the security audit scan (column 7, lines 47-56).

20. Regarding claim 6, Fudge teaches wherein when the central computer performs the operation in which the central computer records the results of the security audit scan, the central computer also copies the results to the database and copies a report to a file system on a database machine when the security audit scan is complete (Figure 1 [blocks 150, 152]; column 3, lines 56-59; column 4, lines 61-67).

21. With regards to claim 26, Todd, Satyavolu, and Fudge do not disclose wherein the result is used for a statistical analysis of security on the remote computer system.

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the result for statistical analysis of security on the remote computer system [Drake, column 1, lines 29-38], since Drake states at column 1, lines 29-38 that such a modification would aid in detecting security flaws as it assumes intrusions and other security problems are rare and that they appear unusual when compared to other user behavior.

23. Claims 7, 8, 10-13, 15, 16, 20, 22, 24, 27-30, 35, 37-39, 41, 44, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Todd in view of Satyavolu.

24. As per claim 7, Todd teaches a method of auditing security of a remote computer system, comprising the steps of:

a. receiving an instruction to perform a security audit scan on the remote computer system (Figures 1, 2 [blocks 34, 36, 38], 3 [block 32, 36], 6, 7, 8; column 4, lines 7-13; column 6, lines 21-26; column 6, lines 50-56);

c. instructing one of the available scanning machines to access the remote computer system via a global computer network to perform the security audit scan of the remote computer system (Figures 6, 7, 8; column 4, lines 14-19; column 7, lines 32-56).

25. Todd does not teach determining which of the plurality of scanning machines is available to perform a security audit scan by examining a schedule for each scanning machine to identify certain ones of the scanning machines that are conducting another security audit scan or are scheduled to conduct another security audit scan, the available scanning machines comprising all of the scanning machines except for the certain scanning machines. It would have been to one of ordinary skill in the art at the time the invention was made to include a determining step to

determine which machine is available to execute the gathering of information [Satyavolu, Figure 1 [block 127], column 6, lines 7-34], since Satyavolu discloses at column 2, lines 26-36 that such a modification would allow a large number of cooperating computer-nodes to fulfill a number of automatically-scheduled and user-initiated data requests in a wholly automated and transparent fashion.

26. Regarding claim 8, Todd teaches the step of recording a result of the security audit scan in a computer memory (column 7, lines 57-65).

27. As per claims 10 and 37, Todd teaches a method of auditing computer system security, comprising the steps of:

a. receiving a schedule request for a security audit scan of a remote computer system, wherein the security audit scan of the remote computer system is scheduled to be conducted after the schedule request is received (Figures 1, 2 [blocks 34, 36, 38], 3 [block 32, 36], 6, 7, 8; column 4, lines 7-13; column 6, lines 21-26; column 6, lines 50-56);

causing the scanning system to establish communication with the remote computer system via a global computer network (Figures 6, 7, 8; column 4, lines 14-19; column 7, lines 32-56); and

causing the scanning system to execute the scheduled security audit scan of the remote computer system via the global computer network (Figures 6, 7, 8; column 4, lines 14-19; column 7, lines 32-56).

28. Todd does not disclose recording the scheduled security audit scan in a database; accessing the database to determine when the scheduled security audit scan of the remote computer system is to be executed; in response to a determination that the scheduled security audit scan of the remote computer system is to be executed in a predetermined period of time (), performing the following steps: i. copying security audit scan data into a scanning system.

29. Satyavolu discloses recording the schedule in a database (column 5, line 54 to column 6, line 6);

accessing the database to determine when the schedule is to be executed (column 6, lines 7-33);

in response to a determination that the function is to be executed in a predetermined time (column 6, lines 35-55, column 8, lines 16-63), performing the following steps:

copying data into a system (column 6, lines 43-55).

It would have been to one of ordinary skill in the art at the time the invention was made to include a scheduling and determining, since Satyavolu discloses at column 2, lines 26-36 that such a modification would allow a large number of cooperating computer-nodes to fulfill a number of automatically-scheduled and user-initiated data requests in a wholly automated and transparent fashion.

30. Regarding claims 11 and 38, Satyavolu discloses the step of receiving at the available scanning machine scan related information for the security audit scan of the remote computer system (column 6, lines 43-67).

31. With regards to claims 12 and 39, Todd discloses wherein the scan related information comprises at least on security assessment to be conducted during the security audit scan (Figures 2, 6, column 6, lines 14-26, column 7, lines 32-56).

32. With regards to claims 13 and 30, Todd teaches wherein the scan related information comprises an identity of at least one remote computer system upon which to conduct the security audit scan (column 6, lines 26-39).

33. Regarding claims 15, 29, and 41, Todd teaches wherein the security audit scan comprises a vulnerability assessment (Figures 2, 6, column 6, lines 14-26, column 7, lines 32-56).

34. Regarding claim 16, Todd discloses wherein the security audit scan comprises a penetration study (Figures 2, 6, column 6, lines 14-26, column 7, lines 32-56).

35. Regarding claims 20, 28, and 44, Satyavolu discloses the step of determining if the available scanning machine is currently conducting the security audit scan on the remote computer system (column 6, lines 7-43).

36. With regards to claims 22, 24, and 46, Todd discloses the step of reporting at least one result of the security audit scan to a user interface (Figures 7 [block 52], 17, column 6, lines 57-67, column 8, line 60 to column 9, line 3).

37. Regarding claim 27, Satyavolu discloses the step of determining which of a plurality of scanning systems is available to perform the scheduled security audit scan by examining a schedule of each of the scanning systems to identify certain ones of the scanning systems that are conducting another security audit scan or are scheduled to conduct another security audit scan, the available scanning systems comprising all of the scanning systems except for the certain scanning systems (column 6, lines 7-55).

38. Regarding claim 35, Satyavolu discloses the step of determining if a request for an immediate security audit scan of one of a plurality of computer systems has been received in response to a determination that the scheduled security audit scan of the remote computer system will be executed outside of the predetermined period of time (column 6, lines 7-55).

39. Claims 17-19, 25, 32-34, 42, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Todd in view of Satyavolu as applied above, and further in view of Fudge.

40. Regarding claims 17, 25, 32, and 42, Todd and Satyavolu do not disclose the step of recording a result of the security audit scan in a database.

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to record the result of the security audit scan in a database [Fudge, Figure 1 [block 152], 2 [block 218], column 3, lines 39-59], since Fudge discloses at column 2, lines 19-28 that such a modification would significantly reduce the time and cost involved in scanning for vulnerable devices by detecting new vulnerabilities to be compared against other shareable devices.

42. With regards to claims 18, 33, and 43, Todd teaches wherein the result comprises at least one vulnerability of the remote computer system detected by the available scanning machine during the security audit scan (Figures 7 [block 52], 17, column 6, lines 57-67, column 8, line 60 to column 9, line 3).

43. Concerning claims 19 and 34, Todd discloses wherein the result further comprises a list of at least one security assessment conducted during the security audit scan (Figures 7 [block 52], 17, column 6, lines 57-67, column 8, line 60 to column 9, line 3).

Conclusion

44. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

45. The following patents are cited to further show the state of the art with respect to security and vulnerability assessment, such as:

United States Patent No. 5,931,946 to Terada et al., which is cited to show network system having external/internal audit system for computer security.

United States Patent No. 6,578,147 B1 to Shanklin et al., which is cited to show parallel intrusion detection sensors with load balancing for high speed networks.

United States Patent No. 6,530,024 B1 to Proctor, which is cited to show an adaptive feedback security system.

United States Patent No. 6,301,668 B1 to Gleichauf et al., which is cited to show adaptive network security using network vulnerability assessment.

United States Patent No. 6,298,445 B1 to Shostack et al., which is cited to show computer security.

United States Patent No. 5,892,903 to Klaus, which is cited to show detecting and identifying security vulnerabilities in an open network.

United States Patent No. 5,032,979 to Hecht et al., which is cited to show distributed security auditing subsystem for an operating system.

United States Patent No. 5,812,763 to Teng, which is cited to show expert system having a plurality of security inspectors for detecting security flaws.

United States Patent No. 6,546,493 B1 to Magdych et al., which is cited to show risk assessment scanning based on detected anomalous events.

46. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

47. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

48. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

49. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

50. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER